Adobe corrige dans l'urgence une faille zero day de Flash

Adobe a posté un correctif de sécurité en urgence de son lecteur Flash, hier mercredi 26 octobre. Un de plus. Il concerne les environnements Windows, Apple (OS X, macOS), Linux et Chrome OS. L'urgence se justifie d'autant que la vulnérabilité est actuellement exploitée, a reconnu l'éditeur. Cette faille zero day *« pourrait permettre à un attaquant de prendre le contrôle du système affecté »*, indique Adobe. Plus précisément, elle s'apparente à une corruption de mémoire qui expose le système et peut mener l'attaquant à exécuter du code à distance sur la machine affectée.

Des attaques, *« limitées »* pour l'heure, ont été constatées sous les environnements Windows 7, 8.1 et 10, indique l'éditeur. Référencée CVE-2016-7855 et rapportée par Neel Mehta et Billy Leonard de Google (Threat Analysis Group), la vulnérabilité touche les versions 23.0.0.185 et antérieures du runtime de Flash pour Windows et Mac, du *player* intégré aux navigateurs Chrome, Edge et Internet Explorer 11, ainsi que celui pour les distributions Linux mais en version 11.2.202.637 et précédentes.

Correction automatique… ou pas

Adobe recommande donc l'installation dans les meilleurs délais de la nouvelle version de son produit : la 23.0.0.205 pour les environnements Mac et Windows, et 11.2.202.643 pour Linux. L'installation devrait s'effectuer automatiquement sous Chrome et les navigateurs de Microsoft à l'occasion de leur prochaine mise à jour. Si l'option de mise à jour automatique est cochée dans le lecteur Flash, tant pour Windows que sur Mac, la correction devrait également s'effectuer automatiquement. Sous Linux, la distribution devrait s'en charger selon la fréquence des mises à jours choisies par l'utilisateur. Sinon, il est conseillé de la faire manuellement en téléchargeant l'application depuis cette page.

Lire également
Mozilla programme l'arrêt prochain de Flash dans Firefox
Google Chrome va bloquer le contenu Flash dès décembre
Adobe Flash signe son grand retour sous Linux